UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/859,429 | 05/18/2001 | Makoto Kayashima | 566.39530VX1 | 5340 |

24956 7590 02/27/2007

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| KHOSHNOODI, NADIA | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 02/27/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/859,429 | KAYASHIMA ET AL. | |
| | Examiner | Art Unit | |
| | Nadia Khoshnoodi | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *8,9 and 11-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-9 and 11-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/761,742.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

Claims 1-7 and 10 are cancelled. Applicant's arguments/ amendments with respect to amended claims 8-9 & 13 and previously presented claims 11-12 filed 11/8/2006 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

### *Response to Arguments*

Applicants contend that Wiegel fails to teach/suggest "providing security control means and means for obtaining status of security of different managed systems and to change configuration of the managed systems for controlling a security both during the design phase and during the operating phase as in the present invention." Examiner respectfully disagrees. Wiegel teaches that each of the available services in the network which are implemented via various network nodes (i.e. "managed system") has their own policy associated with it as designated by a user (col. 15, lines 57-63 and col. 17, lines 22-40), i.e. providing/controlling security during the design phase. Wiegel further teaches that all of the security policies derived for the nodes in the network are then implemented when the firewall of the entire system (i.e. "information system") is instructed to enforce those policies defined for the nodes, i.e. controlling security during the operation phase (col. 15, lines 63-67). Still further, Wiegel teaches that each packet received is checked by the firewall, which enforces the various rules set forth by each of the managed systems' security policy. Once the packet is evaluated, it is either accepted, rejected, or taken to another level for further processing so as to result in maintaining the managed systems' security

status, i.e. a means (audit programs) for obtaining status of security of different manages systems (col. 16, line 57 – col. 17, line 20). Finally, Wiegel teaches that the policy may be edited at any time, as designated by a user, i.e. changing configuration of the managed system to control security of the managed system during the operating phase (col. 16, lines 1-25).

Applicants further contend that Wiegel fails to teach/suggest "a security design step for designing security specification to be applied to the information system by extracting an information security policy which corresponds to each managed system constituting an information system designated by a user from a database where a correspondence between information security policies representing policies of security measures with at least one managed system and the managed system is described." Examiner respectfully disagrees. Wiegel teaches that a user may choose to implement a security policy per node of the network that is intended to provide some type of service by using various icons that represent various rules, i.e. a security design step for designing security specification to be applied to the information system by extracting an information security policy which corresponds to each managed system (col. 12, lines 31-48, col. 13, lines 38-51, and col. 14, lines 1-19). Wiegel also teaches that once a security policy is created for each of the network nodes which have specific rules to implement, the firewall is instructed to enforce these rules based on each of the nodes security policies, i.e. security specification to be applied to the information system by extracting an information security policy which corresponds to each managed system constituting an information system designated by a user from a database where a correspondence between information security policies representing policies of security measures with at least one managed system and the managed system is described (col. 15, lines 63-67 and col. 22, lines 24-

30). Thus, Wiegel teaches a security design step for designing security specification to be applied to the information system by extracting an information security policy which corresponds to each managed system constituting an information system designated by a user from a database where a correspondence between information security policies representing policies of security measures with at least one managed system and the managed system is described.

Still further, Applicants contend that Wiegel fails to teach/suggest "a security install step for executing a plurality of audit programs wherein a process is described to audit security status concerning the information security policy which is specified by the security specifications designed in the security design step, for collecting the security status of each managed system designed by the user, and for changing the security status of the managed systems designated by the user, based on the collected information in consistency of information security policies specified by the securities specification designed in the security design step." Examiner respectfully disagrees. Wiegel teaches that as each packet arrives at the firewall, the firewall evaluates the packet in accordance with a security policy designed for the managed system the packet is intended for, where this packet is either accepted, rejected, or subjected to further processing, i.e. a security install step for executing a plurality of audit programs wherein a process is described to audit security status concerning the information security policy which is specified by the security specifications designed in the security design step (col. 10, lines 1-41, col. 13, lines 60-67, col. 15, lines 63-67, and col. 22, lines 24-30). Wiegel further teaches that a centralized database maintains system event information, as well as that the system may include a monitor agent which has the responsibility of "monitoring, reporting, and notification about the security status" of the nodes/agents in that network which surround the knowledge base, i.e.

audit security status concerning the information security policy which is specified by the security specifications designed in the security design step, for collecting the security status of each managed system designed by the user, and for changing the security status of the managed systems designated by the user (col. 11, lines 25-65). Finally, Wiegel teaches that the policy of each of the managed systems may be changed to extend commands or add new policies based on the services being provided, where these changes are only made if they are verified as falling within the limits of the originally created security policy (col. 14, lines 20-61, col. 19, line 26 – col. 20, line 45, col. 31, lines 36-60). Thus, Wiegel teaches a security install step for executing a plurality of audit programs wherein a process is described to audit security status concerning the information security policy which is specified by the security specifications designed in the security design step, for collecting the security status of each managed system designed by the user, and for changing the security status of the managed systems designated by the user, based on the collected information in consistency of information security policies specified by the securities specification designed in the security design step.

Finally, Applicants contend that Wiegel fails to teach/suggest "a security management step for executing the install step periodically." Examiner respectfully disagrees. Wiegel teaches that the auditing occurs for every packet that is received by the firewall (where there is more than one packet received by the firewall on a regular basis), i.e. a security management step for executing the install step periodically (col. 13, lines 57-67 and col. 17, lines 3-10). Thus, Wiegel teaches a security management step for executing the install step periodically.

Examiner would like to point out that the Wiegel reference, based on the broadest reasonable interpretation of the claim language (MPEP 2111), has not been overcome. For

example, the term "security status" is broad (in the manner that it is claimed) and thus is interpreted as any security information associated with the managed system. In another example, the term "periodically" as used in reference to applying the install step is also broad and is therefore broadly interpreted.

If Applicants believe the claimed language still distinguishes over the cited prior art of record (after reviewing the Examiner's interpretation of the claim language and the cited reference), they are encouraged to explain in detail which specific limitation they feel is not found in Wiegel. Also, if the Applicants wish to schedule an interview, they should have the Attorney of Record call the Examiner to set up a convenient date/time in order to discuss the claim language/cited prior art in more detail.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. Wiegel teaches the limitations that Applicants suggest distinguish from the prior art. Furthermore, the cited prior arts in combination with Wiegel teach the limitations not explicitly disclosed by Wiegel. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 11-12:

These claims recite the limitation "said management program," "the management program," "said security diagnose step," and "said audit/management program" in various lines of the claims. Since claim 8 was amended to remove the portion which introduced a management program and a security diagnose step, there is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 102***

I. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

II. Claims 8-9, 11, and 13 are rejected under 35 U.S.C. 102(e) as being fully anticipated by Wiegel United States Patent No. 6,484,261.

As per claims 8 and 13:

Wiegel teaches a security design step for designing security specification to be applied to the information system by extracting an information security policy which corresponds to each managed system constituting an information system designated by a user from a database where a correspondence between information security policies representing policies of security measures with at least one managed system and the managed system is described (col. 12, lines 31-48, col. 13, lines 38-51, and col. 14, lines 1-19); a security install step for executing a

plurality of audit programs wherein a process is described to audit security status concerning the information security policy which is specified by the security specifications designed in the security design step, for collecting the security status of each managed system designed by the user (col. 10, lines 1-41 and col. 13, lines 60-67), and for changing the security status of the managed systems designated by the user, based on the collected information in consistency of information security policies specified by the securities specification designed in the security design step (col. 11, lines 30-48, col. 14, lines 53-61, and col. 16, lines 9-34); and a security management step for executing the install step periodically (col. 17, lines 5-10).

As per claim 9:

Wiegel teaches the security management method of claim 8. Furthermore, Wiegel teach the security management method wherein said security install step comprises a diagnosis step for diagnosing the security of the information system designated by said user by extracting the audit program made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications designed in said security specification design step from a database where a correspondence is described of the information security policy (col. 10, lines 1-41), the managed system and the audit program where a process is written to audit security status concerning said information security policy of said managed system, and executing (col. 11, lines 31-48); and a change step, wherein the management programs, made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications designed in said security specification design step, are extracted from a database describing a correspondence of the information security policy, the managed system and the management program describing a processing for controlling the

security status concerning the security policy, the managed system and said information security policy of a security of said managed system, and the management program designated by the user is extracted among the extracted programs to be executed, to allow the security status of the managed system corresponding to the extracted management program to adjust to the information security policy corresponding to the management program (col. 19, line 26 – col. 20, line 45 and col. 22, lines 24-30).

As per claim 11:

Wiegel teaches the security management method of claim 8. Furthermore, Wiegel teaches the method wherein, in accordance with setting a content received from the user, said management program changes the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program (col. 16, lines 9-34).

***Claim Rejections - 35 USC § 103***

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

IV. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel United States Patent No. 6,484,261 as applied to claim 8 above and further in view of CERT's CC Vendor-Initiated Bulletins 1994-1998.

As per claim 12:

Wiegel substantially teaches the security management method, wherein a diagnosis results obtained in said security diagnose step which is executed for the information system designated by the user are reflected in the database describing the correspondence of the information security policy with at least one managed system and an audit/management program stored so as to correspond to each set of the information security policy and the managed system as applied to claim 8 above. Not explicitly disclosed is security hole information published by a security information organization including CERT or Computer Emergency Response Team. However, CERT/CC Vendor–Initiated Bulletins disclose security hole information published by a security information organization including CERT. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wiegel to incorporate the use of security hole information published by a security information organization including CERT or Computer Emergency Response Team. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since CERT/CC Vendor –Initiated Bulletins 1994-1998 suggest that it is very important to deal with security vulnerabilities as soon as possible which means that it is necessary to report vulnerabilities as discovered in order to allow all users to take the necessary precautions in pages 1-8.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,990,591
2. US Patent No. 7,020,697
3. US Patent No. 6,115,735
4. US Patent No. 6,216,231
5. US Patent No. 6,678,827

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
2/22/2007

NK

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100